OCRA: Othello Contracts Refinement Analysis
Version 1.3

Alessandro Cimatti, Michele Dorigatti, Stefano Tonetta*

Abstract

Contract-based design enriches a component model with properties structured in pairs of assumptions and guarantees. These properties are expressed in term of the variables at the interface of the components, and specify how a component interacts with its environment: the assumption is a property that must be satisfied by the environment of the component, while the guarantee is a property that the component must satisfy in response. Contract-based design has been proposed in many methodologies for taming the complexity of embedded systems. In fact, contract-based design enables stepwise refinement, compositional verification, and reuse of components.

OCRA (Othello Contracts Refinement Analysis) is a tool that provides means for checking the refinement of contracts specified in a linear-time temporal logic. The specification language allows to express discrete as well as metric real-time constraints. The underlying reasoning engine allows checking if the contract refinement is correct. OCRA has been used in different projects and integrated in tools.

This document provides a manual on how to use OCRA, specifically its input language and its commands.

Contents

1 Introduction **3**

2 Input language **3**
- 2.1 Components . . . 3
- 2.2 Hybrid vs. Discrete Time . . . 4
- 2.3 Interface . . . 4
  - 2.3.1 Ports . . . 4
  - 2.3.2 Parameters . . . 5
  - 2.3.3 Operations . . . 5
  - 2.3.4 Defines . . . 5
  - 2.3.5 Contracts . . . 5
- 2.4 Refinement . . . 5
  - 2.4.1 Subcomponents . . . 5
  - 2.4.2 Connections . . . 6
  - 2.4.3 Constraints . . . 6
  - 2.4.4 Validation Properties . . . 7
  - 2.4.5 Asynchronous vs. Synchronous Refinement . . . 8
  - 2.4.6 Contracts refinement . . . 8
- 2.5 Constraint language . . . 8

3 Verification of Contracts Refinement **9**

4 Integration with NUXMV for Compositional Modeling and Verification **10**

*For a bug report, a feature request or other suggestions, please send email to `ocra@list.fbk.eu`.

5 Advanced features **12**
5.1 Verification of Receptiveness . . . 12
5.2 Contract-based Safety Analysis . . . 12

6 Interactive Commands of OCRA **13**

7 OCRA Command Line Options **24**

A Concrete syntax **26**
A.1 Othello System Specification . . . 26
A.2 Othello Port Types . . . 27
A.2.1 Boolean . . . 27
A.2.2 Enumeration Types . . . 27
A.2.3 Word . . . 27
A.2.4 Integer . . . 27
A.2.5 Real . . . 27
A.2.6 Continuous . . . 27
A.2.7 Array . . . 27
A.2.8 Uninterpreted functions . . . 28
A.3 Othello constraints . . . 28

B Abstract syntax and semantics **29**
B.1 Abstract syntax and semantics of HRELTL constraints . . . 29
B.1.1 Abstract syntax . . . 29
B.1.2 Semantics . . . 30
B.1.3 Examples . . . 31
B.2 Abstract syntax and semantics of the system specification . . . 31

C Patterns **32**

1 Introduction

OCRA is a tool that provides automated support for contract-based design with temporal logics. OCRA relies on the contract framework originally proposed in [CT12, CT], where assumptions and guarantees are specified as temporal formulas.

The main functionality of OCRA is the verification of the contract refinement. OCRA checks if a given contract refinement is correct, generating the corresponding set of proof obligations and checking their validity. OCRA takes as input a textual description of the components interfaces and their decomposition into sub-components, the components' contracts and their refinement with the contracts of the sub-components. The OCRA input file, also called OSS (OCRA System Specification), describes a tree of components (given by the decomposition into sub-components), which represents the system architecture.

The contracts are specified in Othello [CRST12], a human-readable language which can be mapped to temporal formulas in the HRELTL [CRT09], and thus represent sets of hybrid traces. The contract refinement is however independent from the nature of the traces and OCRA provides an option to interpret the contracts over discrete-time traces restricting the input to forbid continuous ports and allow LTL [Pnu77] contracts only.

In order to prove the validity of the proof obligations deriving from contract refinement, OCRA interacts with NuSMV3 [NuS], a framework that includes nuXmv [nuX], HyCOMP [HyC], and xSAP [XSA]. NUSMV3 provides the functionality to either prove that the formulas are valid, or to find counterexamples, which can be inspected by the user in order to find the bugs in the contract refinement. When the contracts are written in the standard discrete-time LTL, to prove or disprove the validity of the proof obligations the BDD-based engine is used. In the general case of HRELTL, reasoning relies on Satisfiability Modulo Theory (SMT). Since logical entailment for HRELTL is undecidable, bounded model checking techniques are used to find counterexamples to the contract refinement [CRT09, CT12].

OCRA has been developed within the European project SafeCer [Saf], focusing on the compositional certification of embedded systems. The tool is publicly available [OCR].

2 Input language[1]

2.1 Components

The main input of OCRA is a textual specification of a system architecture and the related contract refinement. The format of this input is the OCRA System Specification (OSS), which contains the specification of components, their ports and contracts, and their decomposition. Each component specification starts with the keyword **`COMPONENT`** and ends with the following **`COMPONENT`** or with the end of the input. For example, the OSS shown in Figure 1 contains three component specifications.

Each component specification contains a name, an interface part (introduced with the **`INTERFACE`**), and optionally a refinement part (introduced with the keyword **`REFINEMENT`**). A component without refinement is called a leaf component. In the interface part, the ports, the parameters, and the contracts are declared. In the refinement part, the subcomponents are declared and the connections and constraints among the ports of the component and subcomponents are specified. Finally, still in the refinement part, the refinement of the component contracts is also specified. In the following section, we detail the syntax of these elements.

One (and only one) of the component specifications is tagged with the keyword **`system`**. We refer to this component as the system component. The system architecture is a tree of component instances where the root is an instance of the system component and each node is either an instance of a leaf component and has no children or has as children the instances specified as subcomponents in the refinement. The system architecture of the example in Figure 1 has three nodes, if `simple_instance` is the name of the root, then `simple_instance.a` and then `simple_instance.b` are the leaves.

[1] The OCRA data types and operators are based on the NUXMV input language. See `https://es.fbk.eu/tools/nuxmv/downloads/nuxmv-user-manual.pdf` for a detailed description.

```
COMPONENT example1 system
 INTERFACE
  INPUT PORT in_data: boolean;
  OUTPUT PORT out_data: boolean;

  CONTRACT reaction
   assume: in the future in_data;
   guarantee: always (in_data implies in the future out_data);

 REFINEMENT
  SUB a: A;
  SUB b: B;

  CONNECTION a.in_data := in_data;
  CONNECTION b.in_data := a.out_data;
  CONNECTION out_data:= b.out_data;

  CONTRACT reaction REFINEDBY a.reaction, b.pass;


COMPONENT A
 INTERFACE
  INPUT PORT in_data: boolean;
  OUTPUT PORT out_data: boolean;

  CONTRACT reaction
   assume: in the future in_data;
   guarantee: always (in_data implies in the future out_data);


COMPONENT B
 INTERFACE
  INPUT PORT in_data: boolean;
  OUTPUT PORT out_data: boolean;

  CONTRACT pass
   assume: true;
   guarantee: always (in_data implies out_data);
```

Figure 1: Simple OSS example

2.2 Hybrid vs. Discrete Time

The semantics of components is defined in terms of traces (see Section B for a formal definition). Traces may be discrete where the model of time is the set of natural numbers or hybrid which combines discrete changes with continuous evolution of time (the time model in this case is the subset of $\mathbb{N} \times \mathbb{R}$ containing $\langle 0, 0 \rangle$ and such that for all $\langle i, t \rangle$, $\langle i', t' \rangle$, if $i < i'$ then $t \leq t'$). The default model is hybrid. In the discrete-time case, the language is syntactically restricted (see Section 2.3.1 and 2.5). The user can require to interpret the model with discrete time by writing at the beginning of the model:

```
@requires discrete-time
```

2.3 Interface

2.3.1 Ports

The component interface contains a (possibly empty) set of port declarations. Each port is declared with the keyword **`PORT`**, preceded by the direction (**`INPUT`**/**`OUTPUT`**) and followed by the name and the type. Allowed types are **`boolean`**, **`integer`**, **`real`**, **`event`**, **`continuous`**, **`signed word`**, **`unsigned word`**, range of integers, list of integers or symbolic constants. In the discrete-time case, **`continuous`** type cannot be used.

2.3.2 Parameters

A component interface may contain also parameters. These are introduced with the **PARAMETER**. The type of parameters can be **boolean**, **integer**, **real**, **signed word**, **unsigned word**, range of integers, list of integers or symbolic constants and uninterpreted functions. Parameters are like input port that do not change value along time. The parameters of subcomponents can be set by the connection (see the example in Figure 3). Therefore the same component can be instantiated with different parameters. Moreover, the value may depend on the parameters of the father component.

Parameters can be declared with the uninterpreted function type. The following code declares a function with two integer arguments and an integer return value:

```
PARAMETER f : integer * integer -> integer;
```

In contracts function will be referenced through calls, with the standard syntax:

```
guarantee : always f(0, 0) > 0;
```

2.3.3 Operations

A special kind of port is called operation. A component can provide an operation or require it from another one. Operations can be seen as a collection of ports: if an operation is declared in a component in the way shown below,

```
PROVIDED OPERATION PORT P (a : boolean, b : real) : boolean;
```

several ports are implicit declared and can be referenced:

```
INPUT P_call : event -- the event corresponding to the call of the operation
INPUT P_a_param : boolean -- the first parameter
INPUT P_b_param : real -- the second parameter
OUTPUT P_ret : event -- the event corresponding to the operation returning
OUTPUT P_ret_value : boolean -- the return value
```

Therefore, the form of an operation is much like a function in a traditional programming language. However, there is no semantic constraints on the implicit ports. A specific semantics should be enforce by means of constraints.

If no return value port is declared if the return type of the operation is void. As for the other ports, if a component is refined in subcomponents, it is possible to define the connections between the operations.

2.3.4 Defines

A define is a kind of macro. Every time a define is met in expressions, it is substituted by the expression associated with this define. Therefore, the type of a define is the type of the associated expression in the current context. Define expressions may contain **next** operators; normal rules apply: no nested **next** operators.

A define is not a port or a parameter, so it cannot be used in the left hand side of a **CONNECTION**.

2.3.5 Contracts

A component interface may contain a set of contracts. Each contract is introduced with the keyword **CONTRACT**, followed by the name of the contract and two constraints (see also Section 2.5) representing an assumption and a guarantee. The assumption is introduced with the keyword **assume** and represents a property that must be satisfied by the environment of the component. The guarantee is introduced with the keyword **guarantee** and represents a property that must be satisfied by the implementation of the component provided that the assumption holds.

2.4 Refinement

2.4.1 Subcomponents

The component refinement contains a set of subcomponent declarations. Each subcomponent is introduced with the keyword **SUB** followed by the name and the type. The type must be the name of another component. However, the type cannot be the refined component or any ancestor in the tree structure of the system architecture.

```
COMPONENT example2 system
 INTERFACE
  INPUT PORT in_data: real;
  OUTPUT PORT positive: boolean;

  CONTRACT positive
   assume: always (in_data>=0);
   guarantee: always positive;

 REFINEMENT
  SUB a: A;
  SUB b: B;

  CONNECTION b.in_data := in_data + a.out_data;
  CONNECTION positive := b.out_data>0;

  CONTRACT positive REFINEDBY a.positive, b.past;


COMPONENT A
 INTERFACE
  OUTPUT PORT out_data: real;

  CONTRACT positive
   assume: true;
   guarantee: always (out_data>0);


COMPONENT B
 INTERFACE
  INPUT PORT in_data: real;
  OUTPUT PORT out_data: real;

  CONTRACT past
   assume: true;
   guarantee: always (out_data<=0 implies in the past in_data<=0);
```

Figure 2: Example with arithmetic expressions in the connections

2.4.2 Connections

The component refinement contains a (possibly empty) set of connections. Each connection connects the output of the component or the input of the subcomponents to an expression over the inputs of the component and the outputs of the subcomponents. The connection is introduced with the keyword **`CONNECTION`**[2] followed by the connected port and the expression. The ports of subcomponents are referred to with the the dot notation (name of the subcomponent followed by `"."` followed by the name of the port). The type of the port and the expression must be the same. So, if the connected port is **`real`**, then also the expression must be a **`real`** expression (see the example in Figure 2).

Remark 1 *The presence of Boolean or arithmetic connectors in the connection may be seen as not a principled design choice, because it hides a component that implements such connector.* OCRA *supports it for flexibility but the user should consider the alternative model where additional components are introduced and all connections are atomic, just connecting one port to another port.*

Remark 2 *In a principled design, every output port of a refined component and every input port of its subcomponents should be connected by a connection. If not, such port is called dangling.* OCRA *warns the user about the presence of such ports but they are supported. The semantics of dangling ports is that their value is non-deterministically chosen. Note that the same behavior can be obtained by adding a subcomponent that generates such non-deterministic value.*

2.4.3 Constraints

The component refinement contains a (possibly empty) set of temporal constraints (see also Section 2.5) on the ports of the component and the ports of the subcomponents. Such constraints are introduced with the **`CONSTRAINT`**.

[2] In the earlier version of the language, connections were named **`DEFINE`**. This is no more supported.

```
COMPONENT example3 system
 INTERFACE
  INPUT PORT x: real;
  OUTPUT PORT alarm: event;
  PARAMETER min_period: real;
  PARAMETER threshold: real;
  CONTRACT alarm
   assume: always (change(x) implies then time_until(change(x))>min_period);
   guarantee: always ((x<=threshold) implies time_until(alarm)<=10);
 REFINEMENT
  SUB d: Device;
  SUB m: Monitor;
  CONNECTION d.x := x;
  CONNECTION alarm := m.out_alarm;
  CONNECTION m.period := (min_period<=2)?min_period:2;
  CONNECTION d.threshold := threshold;
  CONSTRAINT always (m.request implies time_until(d.request)<=3);
  CONSTRAINT always (d.alarm implies time_until(m.in_alarm)<=3);
  CONTRACT alarm REFINEDBY d.alarm, m.alarm, m.request;
  CONSISTENCY NAME c1 := example3.alarm.ASSUMPTION, d.alarm.ASSUMPTION, m.request.ASSUMPTION;
  POSSIBILITY NAME p1 := example3.alarm.GUARANTEE GIVEN d.alarm.ASSUMPTION, m.request.ASSUMPTION;
  ENTAILMENT  NAME e1 := m.request.GUARANTEE BY m.request.ASSUMPTION;

COMPONENT Device
 INTERFACE
  INPUT PORT x: real;
  INPUT PORT request: event;
  OUTPUT PORT alarm: event;
  PARAMETER threshold: real;
  CONTRACT alarm
   assume: true;
   guarantee: always ((request and x<=threshold) implies time_until(alarm)<=1);

COMPONENT Monitor
 INTERFACE
  INPUT PORT alarm: event;
  INPUT PORT in_alarm: event;
  OUTPUT PORT request: event;
  OUTPUT PORT out_alarm: event;
  PARAMETER period: real;
  CONTRACT request
   assume: true;
   guarantee: (time_until(request)<=period) and
              (always (request implies then time_until(request)<=period));
  CONTRACT alarm
   assume: true;
   guarantee: always (in_alarm implies time_until(out_alarm)<=1);
```

Figure 3: More complex OSS example

Constraints may be useful to model special kind of connections, such lossy channels or delays (see the example in Figure 3).

Remark 3 *Also in this case, the use of constraint may be avoided by introducing a component implementing the special connection (see also Remarks 1 and 2).*

2.4.4 Validation Properties

The component refinement contains a (possibly empty) set of validation properties on a contract refinement. There are three types of validation properties that can be defined: *consistency*, *possibility*, and *entailment*. In their definitions, formula ids are used to make reference to assumption, guarantee, and norm guarantee [3] of the contracts of components. A formula id is made up of a component name, a contract name and one of the keyword: **ASSUMPTION**, **GUARANTEE**, or **NORM_GUARANTEE**. These three parts are separated using the dot notation (see below an example).

Let us now explain the three type of validation properties:

[3] Norm guarantee is defined as $A \rightarrow G$, where A is the assumption and G is the guarantee of a given contract.

- *Consistency:* this type of validation property aims at formally verifying the absence of logical contradictions of a given subset of properties (assumption, guarantee, and norm guarantee of the contracts on a refined component and its subcomponents). It is possible to define a consistency property in the following form:
CONSISTENCY NAME name := $prop_0, \ldots, prop_n$, where $prop_0, \ldots, prop_n$ is a list of formula ids.

- *Possibility:* this kind of validation property allows to verify whether a property is consistent with a set of other properties specified in the contracts. It is possible to define a possibility property in the following form:
POSSIBILITY NAME name := $prop_0$ **GIVEN** $prop_1, \ldots, prop_n$, where $prop_0$ can be a formula or a formula id, and $prop_1, \ldots, prop_n$ is a list of formula ids.

- *Entailment:* this type of validation property aims at verifying whether an expected property is implied by a set of other properties specified in the contracts. It is possible to define a possibility property in the form:
ENTAILMENT NAME name := $prop_0$ **BY** $prop_1, \ldots, prop_n$, where $prop_0$ can be a formula or a formula id, and $prop_1, \ldots, prop_n$ is a list of formula ids.

As we mentioned above, a formula id is made up of a component name, a contract name and one of the keyword: **ASSUMPTION**, **GUARANTEE**, or **NORM_GUARANTEE**. These three parts are separated using the dot notation. For example, the formula id corresponding to the `assumption` of the contract `alarm` on component `example3` in Figure 3 is denoted as: example3.alarm.ASSUMPTION. We remark that formula ids used in the definition of any validation properties can only make reference to contracts on the component where is defined the validation property and its subcomponents.

2.4.5 Asynchronous vs. Synchronous Refinement

The semantics of the composition of subcomponents is synchronous. This means that subcomponents progress simultaneously. At every discrete step or time evolution, every component behaves as specified by the contracts. It is possible to specify an asynchronous composition by using the keyword **ASYNC** in front of the keyword **REFINEMENT**. In this case, at every discrete step, each component either behaves as specified by the contracts or *stutters*. The relationship between the stuttering of one component and the other events must be specified with a **CONSTRAINT** using the implicit event **stutter**. For example, a constraint may force a component to stutter when the other component it is performing an event. See the examples in the distribution of the tool. By default, no fairness is introduced to avoid endless stuttering of a component. By setting the option ocra_async_fairness the tool will introduce such constraint.

2.4.6 Contracts refinement

In the component refinement, each contract present in the component interface should be refined by some contracts of the subcomponents. This relationship is introduced with the keyword **REFINEDBY** preceded by the name of the refined contract followed by a list of contracts of the subcomponents. These are referred to with the the dot notation (name of the subcomponent followed by **"."** followed by the name of the contract).

2.5 Constraint language

OCRA input language uses OTHELLO [CRST12] to specify contracts. In the discrete-time case, it coincides with LTL and is interpreted over discrete traces.

The relevant syntax of OTHELLO has been summarized in Table 1 together with the corresponding mathematical formulation in HRELTL (see Section B for a formal definition of syntax and semantics).

In case of discrete time, **der** and **time_until** are not allowed.

Basic formulas are defined with linear arithmetic predicates over the variables or their derivatives. For examples, `x-e<limit` and **der**`(x)<0` are well-defined formulas. Predicates can be combined with Boolean and temporal operators. For example, `x-e<limit` **and der**`(x)<0` and **always** `x-e<limit` are well-defined formulas.

In temporal logic, a formula without temporal operators is interpreted in the initial state. Thus, `x=0` characterizes all traces that start with a state evaluating `x` to 0, and then `x` can evolve arbitrarily. Instead, to express that a predicates holds along the whole evolution, one may use the **always** operator as in **always** `x=0`.

Table 1: The OTHELLO constraints language grammar.

constraint	:=	*atom* |	ϕ	:=	a |
		not *constraint* |			$\neg\phi$ |
		constraint **and** *constraint* |			$\phi \wedge \phi$ |
		constraint **or** *constraint* |			$\phi \vee \phi$ |
		constraint **implies** *constraint* |			$\phi \rightarrow \phi$ |
		always *constraint* |			$G\phi$ |
		never *constraint* |			$G\neg\phi$ |
		in the future *constraint* |			$F\phi$ |
		constraint **until** *constraint*;			$\phi\, U\phi$;
atom	:=	**true** |	a	:=	$\top$ |
		false |			$\bot$ |
		term relation term |			$t \bowtie t$ |
		time_until(*term* **)** *relation term* |			$\rhd_{\bowtie t} t$ |
		change(*port* **)** |			$v' \neq v$ |
		term ;			t;
term	:=	*port* |	t	:=	v |
		constant |			c |
		term function term |			$t \star t$ |
		der(*port* **)** |			$\dot{v}$ |
		next(*port* **)** ;			v';

Another classical example of properties is the response to a certain event. The formula **always** (p **implies in the future** q) defines the set of traces where every occurrence of p is followed by an occurrence of q. Note that q may happen with a certain delay (although there is no bound on such delay). The formula **always** (p **implies** q) instead forces q to happen at the instant of p.

The above formulas do not constrain the time model of the traces. Therefore, they can be interpreted either as discrete traces or as hybrid traces. However, the logic is suitable to characterize specific sets of hybrid traces, constraining when there should be discrete events and how the continuous variables should evolve along continuous evolutions.

The **der**(.) operator is used to specify constraints on the derivative of the continuous evolution of continuous variables. For example, the following OTHELLO constraint:

```
always (train.location<=target implies der(train.location)>=0)
```

characterizes the set of hybrid traces where in all states, if the train has not yet reached the target location, its speed (expressed as the derivative of the location) is greater than or equal to zero.

The **next**(.) operator is used to specify functional properties requiring discrete changes to variables. For example, we can express the property that the warning variable will change value after the train's speed passes the limit with the following constraint:

```
always (speed>limit implies
                    in the future next(warning)!=warning)
```

The expression **change**(x) can be used instead of **next**(x)!=x.

In order to constrain the delay between two events, we use the **time_until**(.) operator, which denotes the time that will elapse until the next occurrence of an event. For example, the formula **always** (p **implies time_until** (q)<max_delay) defines the set of hybrid traces where p is always followed by q in less than max_delay time units.

3 Verification of Contracts Refinement

The contract refinements specified in the OSS be seen as a set of proof claims that are resolved by the tool. The claim say 1) that if the subcomponents satisfy their contracts, then also the composite component satisfies its contracts, and 2) that if the subcomponents satisfy their contracts and the environment of the composite component satisfies the related assumptions, then also the assumptions of each subcomponents are satisfied.

The OCRA command to check the refinement of contracts is `ocra_check_refinement`. See Section 6 for a complete description of options. The command internally processes the input, generates the proof obligations corresponding to the proof claims, and check their validity. It reports the results to standard output, detailing for each proof claim if the claim is correct and if not, it produces a counterexample trace witnessing that the claim is wrong.

A typical usage of the tool is the following. First, the user writes the OSS in a textual file. The typical suffix used for these files is `.oss` (for example `example1.oss`). Emacs users can use the OCRA mode for syntax highlighting (see `ocra-mode.el` file provided with the tool distribution). Second, OCRA must be run in interactive mode with the command `ocra -int`. Before checking the refinement, the user may check the syntax of the input by calling `ocra_check_syntax -i example1.oss`. OCRA provides also a simple validation check that verifies if each constraint in the contracts is satisfiable. This can be performed with the command `ocra_check_consistency`. Finally, after syntax checking and validation, the user may run the actual verification with the command `ocra_check_refinement`. The overall sequence therefore is:

```
$ ocra -int
ocra > ocra_check_syntax -i example1.oss
ocra > ocra_check_consistency
ocra > ocra_check_refinement
```

4 Integration with NUXMV for Compositional Modeling and Verification

When considering discrete-time behaviors, OCRA is tightly integrated with the nuXmv model checker to model and verify behavioral models that implement the OCRA components. The behavior of components can therefore described in the SMV language (the input language of NuSMV and nuXmv). In SMV, the behavior is described by means of logical formulas that describe the initial states and the state transitions. An SMV specification can be organized by modules, but the language does not allow to have a component-based specification with a clear definition of the component interfaces. In fact, in the discrete-time case, OCRA can be used even without contracts just to specify SMV in a component-based fashion. Figure 4 shows in a nutshell three different scenario of modeling and verifying SMV models: in the first, scenario only the SMV language and the nuXmv model checker is used; in the second scenario, the system architecture is specified in OSS (even without contracts), the behavior of the leaf component is specified in SMV, OCRA generates the SMV of the system composing the leaves according to the architecture, and finally nuXmv is used to verify the model as a whole; in the third scenario, contracts are also specified in the OSS model and OCRA is used for a composition verification.

In order to support this usage, several commands of OCRA take as input or return as output SMV models. These models represent an instantiation of the OCRA component in a free environment. They contain a module corresponding to the OCRA component and a module main instantiating the component.

Going to the detailed syntax, other than being valid SMV models[4], to be used with OCRA, these models need to follow the syntax described below. When starting to model the implementations of an OCRA specification, it is possible to automatically generate the correct structure, using the command `ocra_print_implementation_template`. Figure 4 shows a simple OCRA component and the corresponding SMV template. Note that OCRA version 1.2.0 and earlier used a different (now deprecated) syntax. If needed, it can be enabled with `set ocra_old_smv_format`.

General rules

- Types are slightly different in OCRA and SMV so that the following correspondence must be followed:
  - OCRA input data port of type X corresponds to SMV variable of type X
  - OCRA output data port of type X corresponds to SMV variable of type X
  - OCRA input event port corresponds to SMV input variable of type boolean

[4] see the nuXmv user manual: `https://es.fbk.eu/tools/nuxmv/downloads/nuxmv-user-manual.pdf`

Use case ID	Modeling	Verification & validation
1	Monolithic: Write the system behavior in SMV.	Monolithic: Verify and validate the SMV model with nuXmv.
2	Compositional: • Write the system architecture in OSS. • Write the behavior of the leaf components in SMV. • Build the SMV system behavior with OCRA.	Monolithic: Verify and validate the SMV model with nuXmv.
3	Compositional: • Write the system architecture in OSS. • Specify also the contracts. • Write the behavior of the leaf components in SMV.	Compositional: • Validate contracts with OCRA. • Verify contract refinement with OCRA. • Verify the contracts on the SMV models with OCRA. • Validate the SMV models with nuXmv.

Figure 4: Three scenarios of usage of nuXmv and OCRA in a nutshell

  - OCRA output event port corresponds to SMV input variable of type boolean
  - OCRA parameter of type X corresponds to SMV frozen variable of type X

  Note that the word ”input” has different meanings.

- Since in SMV there is no distinction between input and output, we use the convention that inputs correspond to variables declared outside the component module and passed to module through MODULE parameters, while outputs correspond to some symbols declared insider the MODULE.

Main SMV module

- For each parameter, there must be a frozen variable (FROZENVAR). This has to be also an actual parameter to the module instance.
- For each input port, there must be a state variable (VAR). This has to be an actual parameter to the module instance as well.
- For each output port, there must be a DEFINE. Its body must be a symbol with the same name in the module “component name”
- There must be a single module instance, of type “component name”.

Component SMV module

- For each input port and parameter, there must be a parameter
- For each output port, there must be a symbol

```
COMPONENT Sensor system

    INTERFACE

        INPUT PORT ib : boolean;
        INPUT PORT ie : event;
        OUTPUT PORT ob : boolean;
        OUTPUT PORT oe : event;
        PARAMETER pb : boolean;
```

```
MODULE main
    VAR
        Sensor_inst : Sensor(pb, ie, ib);
    VAR
        ib : boolean;
    IVAR
        ie : boolean;
    FROZENVAR
        pb : boolean;
    DEFINE
        oe := Sensor_inst.oe;
        ob := Sensor_inst.ob;

MODULE Sensor(pb, ie, ib)
    VAR
        ob : boolean;
    IVAR
        oe : boolean;
```

Figure 5: A simple OCRA component and corresponding SMV template

5 Advanced features

5.1 Verification of Receptiveness

For compositionality of a component with its environment, it is necessary that the component does not block inputs from the environment. Since we are in the contract-based framework, it is sufficient to consider only environments satisfying the assumptions of the component contracts. This check is performed automatically by OCRA with the command `ocra_check_receptiveness`. However, the command is limited to consider only assumptions that predicate over the input ports.

5.2 Contract-based Safety Analysis

A specific safety analysis can be performed exploiting the contract-based design and identifying the component failures as the failure of its implementation in satisfying the contract. When the component is composite, its failure can be caused by the failure of one or more subcomponents and/or the failure of the environment in satisfying the assumption. This dependency can be automatically computed based on the contract refinement. The OCRA command `ocra_compute_fault_tree` produces a fault tree in which each intermediate event represents the failure of a component or its environment and is linked to a Boolean combination of other nodes; the top-level event is the failure of the system component, while the basic events are the failures of the leaf components and the failure of the system environment (see [BCMT14] for more details).

6 Interactive Commands of OCRA

ocra_check_refinement - *Checks the contract refinement of the OSS* Command

```
ocra_check_refinement [-C <string>] [-h] [-i <file>] [-k <int>] [-a <string>]
[-f text|xml ] [-o <file>]  [-s]
```

First, it checks the syntax of a model. In case of error, a message is given. Second, it checks that a given system architecture is correct with respect to the specified refinement of contracts. The verification guarantees that if the implementations of the leaf components are correct, then for every composite component C:

- every contract of C is satisfied by the implementations of the subcomponents of C
- every assumption of a subcomponent of C is satisfied by the implementations of the other subcomponents of C or by the environment of C.

If the check finds that the refinement is wrong, the system gives you a counterexample. In case that option `-s` is given, a summary of the checks is provided hiding the formula(s) and description of the trace(s).

Currently, past operators and option bmc_force_pltl_tableau are not supported are not supported with the bmc engine with discrete time interpretation.

Command Options:

`-C <string>`	Check just the specified contract, rather than all of them
`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-k int`	Set the BMC length
`-a string`	Force algorithm type. Valid values are: bmc, bdd, ic3, auto [default=auto]
`-f string`	Selects output format. Valid values are: text, xml [default=text]
`-o <file>`	Set the output file [default=stdout]
`-s`	Prints summary of the results

ocra_check_implementation - *Verifies if an SMV model satisfies the contracts defined in the OSS model* Command

```
ocra_check_implementation -I <file> [-C <string>] [-h] [-i <file>] [-c <name>]
[-k <int>] [-l <int>] [-a <string>] [-f (text|xml)] [-o <file>]
```

Given a finite state machine modeled in the SMV language, and an Othello System Specification, verifies if the machine satisfies the contracts defined in the OSS. At the moment, the command can be used only with propositional models.

Command Options:

`-I file`	Reads the SMV specification
`-C <string>`	Check just the specified contract, rather than all of them

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-l <int>`	bound of K-Liveness [default=10]
`-c string`	Specify the component to be checked
`-k string`	Using bmc algorithm:set the bound on length of path [default=10]. Using ic3 or kzeno: set the bound of underlying IC3 [default=10]
`-a string`	Force algorithm type. Valid values are: bmc, bdd, ic3, auto [default=auto]
`-f string`	Selects output format. Valid values are: text, xml [default=text]
`-o <file>`	Set the output file [default=stdout]

ocra_check_syntax - *Parses an OSS specification and type checks it* Command

```
ocra_check_syntax (-i <file> | -p <string>) [-h] [-C]
```

It checks the syntax of a model.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-p <string>`	Read the specification from a string
`-C`	Consider the specification as an assertion [default=no] (rather than a whole OCRA system specification) Equivalent to deprecated -c

go_ocra - *Parses an OSS specification and type checks it* Command

```
go_ocra [-h] [-i <file>]
```

Parses the model and performs syntactic checks over it.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input

ocra_print_system_implementation - *Compute and prints a system implementation* Command

```
ocra_print_system_implementation [-h] [-i <file>] [-L] [-m <file>] [-o <file>]
```

Given an OSS specification, a set of SMV files and a configuration file with a map between component names and the smv file representing their implementation, outputs a single SMV file for the system implementation.

It requires ocra_discrete_time to be enabled. The configuration file looks like this:

Hydraulic Hydraulic.smv
Select_Switch Select_Switch.smv
subBSCU subBSCU.smv

That is, a line for each space separeted association.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-L`	Disable printing of the contracts [default=enabled]
`-m file`	Reads the file with the map (component name, component smv implementation file)
`-o file`	Outputs the system implementation on file. If not specified, it prints to standard output

ocra_check_consistency - *Check if the contracts of the whole specification are satisfiable* Command

```
ocra_check_consistency [-h] [-i <file>] [-j]
```

By default, it checks every assertion (assumption and guarantee) for being consistent, that is, satisfiable. Alternatively, if the option -j is given, it performs richer checks:

- For each contract, it checks consistency of the conjunction of its assumption and guarantee. Notice that this check subsumes the one by default.
- For each composite component C, checks consistency among assumption of C and assumptions and guarantees of all subcomponents.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-j`	For each contract, checks consistency of the conjunction of its assumption and guarantee and for each composite component C, checks consistency among assumption of C and assumptions and guarantees of all subcomponents

ocra_check_validation_prop - *Check validation properties* Command

```
ocra_check_validation_prop [-h] -i <file> [-a <string>] [-w ] [-P <string>]
                           [-s]
```

By default, it check all validation properties defined in the input specification. Moreover, the validation properties defined in each refined component will be performed on it and its children in isolation. Alternatively, if the option `-w` is given, it checks all validation properties (consistency, possibility, and entailment) considering the entire architecture. In more details, the user can define some constraints on the architecture, for example on the input of the components like setting an input into a constant from the father refinement. So, enable this option `-w`, the check will consider all constrains defined on the architecture contrary to the default case. We remark that the generated additional checks for the different instances in the architecture using option `-w` are not stored in the data base of properties. Finally, if option `-s` is given, a summary of the checks is provided hiding the formula(s) and description of the trace(s).

At the moment, the command can be used only for discrete time.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-a string`	Force algorithm type. Valid values are: bmc, bdd, ic3, auto [default=auto]
`-w`	The whole architecture is considered for the checks
`-P "name"`	Checks only the validation property with the given `name`
`-s`	Prints summary of the results

ocra_check_receptiveness - *Verifies if an SMV model is compatible with every environment satisfying the assumption of the contracts* — Command

```
ocra_check_receptiveness -I <file> [-h] [-i <file>] [-c <name>]
```

Given a finite state machine modeled in the SMV language, and an Othello System Specification, verifies if the machine is compatible with every environment satisfying the assumption of the contracts defined in the OSS. At the moment, the command can be used only with propositional models.

Command Options:

`-I file`	Reads the SMV specification
`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-c string`	Specify the component to be checked

ocra_check_composite_impl - *Check the system implementation compositionally or monolithically* — Command

```
ocra_check_composite_impl -m <file> [-C <string>] [-h] [-a <string>] [-f <string>]
[-i <file>] [-k <int>] [-l <int] [-L] [-M] [-o <file>] [-R] [-s <file>] [-S
<string>]
```

It checks the correctness of the system implementation with a *compositional* strategy by checking:

1. the contract refinement
2. the implementation of each leaf component

Equivalent to issue ocra_check_refinement and ocra_check_implementation on each leaf component.

Alternatively, if the option -M is given, it checks the correctness of the system implementation with a *monolithic* strategy. It computes the system implementation out of the leaf components and the system architecture and it checks its correctness. Equivalent to issue ocra_print_system_implementation and ocra_check_implementation.

Command Options:

`-m file`	Reads the file with the map (component name, component smv implementation file)
`-C <string>`	Check just the specified contract, rather than all of them
`-h`	Shows a brief description of the available options.
`-a string`	Force algorithm type. Valid values are: bmc, bdd, ic3, auto [default=auto]
`-f string`	Selects output format. Valid values are: text, xml [default=text]
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-k int`	Set the BMC length
`-l <int>`	bound of K-Liveness [default=10]
`-L`	Disable printing of the contracts [default=enabled]
`-M`	Perform a monolithic verification by building the system implementation
`-o <file>`	Set the output file [default=stdout]
`-R`	Skip the refinement check
`-s <file>`	Set the output file for the system component [default=None]
`-S <file>`	Select which checks are performed on the leaves [default=implementation] Valid values are full, implementation, none, receptiveness

ocra_print_implementation_template - *Prints the SMV templates of the leaf components* Command

```
ocra_print_implementation_template [-h] [-i <file>] [-L] [-m <file>]
```

The purpose of this command is to aid the modelling of the implementations of the basic (leaf) components of a system.

It generates one o more SMV files, each of them representing the implementation of a leaf component. The generated models are templates: they contain just the language of the component.

If `-m` is given, only the listed components are processed and the SMV files are named according to the mapping. Otherwise, all the leaf components are processed and the SMV files are named after the name of the components.

The configuration file looks like this:
Hydraulic Hydraulic.smv
Select_Switch Select_Switch.smv
subBSCU subBSCU.smv

That is, a line for each space separated association.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-L`	Disable printing of the contracts [default=enabled]
`-m file`	Reads the file with the map (component name, component smv implementation file)

ocra_write_anonymized_models - *Prints the SMV templates of the leaf components* Command

```
ocra_write_anonymized_models [-h] [-i <file>] [-m <file>] [-d <file>]
```

The configuration file looks like this:
Hydraulic Hydraulic.smv
Select_Switch Select_Switch.smv
subBSCU subBSCU.smv

That is, a line for each space separated association.

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-m file`	Reads the file with the map (component name, component smv implementation file)
`-d file`	Reads the file with the map (component name, component smv implementation file)

ocra_print_proof_obligations - *Prints on files the proof obligations composing the refinement check* Command

```
ocra_print_proof_obligations[-h] [-i <file>] [-o <file>]
```

It computes the proof obligations that compose the refinement check and prints them as SMV files, if discrete time interpretation is selected, as HRELTL files otherwise. Trivial proof obligations are not printed.

If -o option is given, its value is used as a prefix that, together with a counter, is used as filename. Otherwise, the filename will follow this format:
$< model > _ < component > _ < contract > _(i|e)[_ < subcontract >]. < extension >$
Where:

- model is the pathname of the input oss
- component is the name of the refined component
- contract is the name of the refined contract
- "i" or "e" stands for the type of the check, that is "implementation" or "environment"
- subcontract, present only for the environment check, is the name of a contract belonging to the refinement of the contract under checking

Command Options:

`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-o file`	Set base output file name

ocra_discrete_time Environment Variable

Interpret the ocra specification over discrete time. Default is false, specification is interpreted over hybrid time.

ocra_make_warnings_errors Environment Variable

Treat every warning as an error. Default is false.

ocra_old_smv_format Environment Variable

Write and read SMV models with the format used before version 1.3.0. Default is false.

ocra_async_fairness Environment Variable

Add to the specification the constraint that each subcomponent will eventually not stutter. It affects only models with asynchronous refinement.

ocra_show_traces - *Shows the traces generated in an ocra session* Command

```
ocra_show_traces [-h] [-v] [-t] [-A] [-m | -o output-file]
[-a | trace_number[.from_state[:[to_state]]]
```

Shows the traces currently stored in system memory, if any. By default it shows the last generated trace, if any. Optional trace number can be followed by two indexes (from_state, to_state), denoting a trace "slice". Thus, it is possible to require printout only of an arbitrary fragment of the trace (this can be helpful when inspecting very big traces). Moreover, the trace descrition also shows information of the component where was generated the trace.

Command Options:

`-h`	Shows a brief description of the available options.
`-v`	Verbosely prints traces content (all state ports, input/output ports, and parameters, otherwise it prints out only the variables that have changed their value from previous state). This option only applies when the Basic Trace Explainer plugin is used to display the trace.
`-t`	Prints only the total number of currently stored traces.
`-a`	Prints all the currently stored traces.
`-m`	Pipes the output through the program specified by the `PAGER` shell variable if defined, else through the UNIX command "more".

`-o output-file`	Writes the output generated by the command to `output-file`.
`trace_number`	The (ordinal) identifier number of the trace to be printed. Omitting the trace number causes the most recently generated trace to be printed.
`from_step`	The number of the first step of the trace to be printed. Negative numbers can be used to denote right-to-left indexes from the last step.
`to_step`	The number of the trace to be printed. Negative numbers can be used to denote right-to-left indexes from the last step. Omitting this parameter causes the entire suffix of the trace to be printed.
`-A`	Prints the trace(s) using a rewriting mapping for all symbols.

ocra_show_property - *Shows the currently stored properties in an ocra session.* Command

```
ocra_show_property [-h] [-v] [[ -c <name> | -a | -g | -q | -r | -s] |
                    [t | f] ] | [-n idx | -P <name>]
```

Shows the properties currently stored in the list of properties. This list is initialized with the properties present in the input file, if any; then all of the properties added by the user with the basic command `ocra_check_syntax` or with any command which requires as input an OSS specification. Generally, three types of properties are distinguished *contracts*, *validation props*, and *proof obligations*. In the last case, the proof obligations are only added to the list of properties through the command `ocra_check_refinement`.

For every property, the following informations are displayed:

- the identifier of the property (a progressive number);
- the property name;
- the property formula;
- the category (ASSUMPTION_PROP, GUARANTEE_PROP, CONSISTENCY_PROP, POSSIBILITY_PROP, ENTAILMENT_PROP, PROOF_OBLIG_PROP, and TRACE_PROP);
- the status of the property (OK, NOT OK, N/A);
- if the formula has been found to be false (true), the index number of the corresponding counterexample (witness) trace;
- the list of traces id that the property is satisfied on each one.
- the list of traces id that the property is not satisfied on each one.

Each property has a name associated except for property with category TRACE_PROP (see command `ocra_check_ltlspec_on_trace`). Validation properties are the only ones that contain a name by definition. On the other hand, for each contract the name for its assumption and guarantee is defined as follows:

$< component > . < contract > .[ASSUMPTION|GUARANTEE]$.

Finally, for each proof obligation, its name is defined as follows:

$< component > . < contract > _(imp|env)[_ < subcontract >]$
Where:

- component is the name of the refined component
- contract is the name of the refined contract
- "imp" or "env" stands for the type of the check, that is "implementation" or "environment"
- subcontract, present only for the environment check, is the name of a contract belonging to the refinement of the contract under checking

By default, all the properties currently stored in the list of properties are shown without printing the formula contents. The option `-v` enable the visualization of the formulas. Specifying the suitable options, properties with a certain category and/or of a certain status (OK or NOT OK), or with a given identifier, or with a given name it is possible to let the system show a restricted set of properties. Moreover, it is possible to show all properties of a given component name. It is allowed to insert several options per category.

Command Options:

`-h`	Shows a brief description of the available options.
`-v`	Verbosely prints formula contents.
`-c <name>`	Prints out the properties of component named "name".
`-a`	Prints only assumption properties.
`-g`	Prints only guarantee properties.
`-q`	Prints only validation properties.
`-r`	Prints only proof obligation properties.
`-t`	Prints only those properties found to be OK.
`-f`	Prints only those properties found to be NOT OK.
`-n idx`	Prints out the property numbered "idx".
`-P <name>`	Prints out the property named "name".
`-s`	Prints the number of stored properties.

ocra_check_ltlspec_on_trace - *Checks whether a property is satisfied on a trace* Command

```
ocra_check_ltlspec_on_trace [-h] [-i] [-n number | -P <name> |
                    [[-c <name>] -p "expr"] ] [-l loopback] trace_number
```

Checks whether a property is satisfied on a given trace. The problem generated can be checked using SAT/SMT backend.

Option `-i` forces the use of the engine for infinite domains. In case the user does not provide this option, a SAT solver is called by default for checking the problem generated if only the formula and trace does not contain infinite precision variables. Otherwise, a SMT solver will be called for solving the problem generated.

We take into account that each OCRA trace may correspond to an infinite number of traces due to the possible presence of more than one loopbacks. So, it is not possible (or at least straightforward) to check all of them. Therefore, we consider just one loopback and provide the user with the possibility to select it.

A `"expr"` to be checked can be specified at command line using option `-p`. This formula is added to the data base of property with the category TRACE_PROP. Each property in the data base is associated with component information, i.e., option `-c` allows to the user to associate `"expr"` with the component information provided. In case the user does not provide this information, the component associated to `"expr"` is the component **`system`** by default.

Alternatively, options `-n` and `-P` can be used for checking a particular formula in the property database. If neither `-n` nor `-p` nor `-P` are used, then each contract (assumption and guarantee) in the OSS specification is checked on the given trace.

The loopback value can be specified at command line using option `-l`. This must a valid `loopback` value on the given trace. If it is not valid, then an error message is printed and also the available loopbacks are provided. In case that option `-l` is not used, then a warning is printed and the check is performed using the first loopback found on the given trace.

Finally, the last argument of the command is the trace number which has to correspond to a trace stored in the system memory. If the trace number is omitted, then an error message is printed. In case that the trace has not loopbacks, then an error message is printed informing the user that the selected trace is finite and cannot satisfy any LTL formula.

Command Options:

`-h`	Shows a brief description of the available options.
`-i`	Forces the use of the engine for infinite domains.
`-c <name>`	Component name to be assigned to the input formula
`-p "expr"`	Checks only the given formula "expr"
`-P <name>`	Checks only the property with the given name
`-n <number>`	Checks only the property with the given index `number` in the property database.
`-l <loopback>`	Checks the property on the trace using `loopback` value. This must a valid `loopback` value on the given trace.
`trace_number`	The (ordinal) identifier number of the trace to be used to check the property. This must be the last argument of the command.

ocra_compute_fault_tree - *Generates a hierarchical fault tree from a contract-based system decomposition* Command

```
ocra_compute_fault_tree [-C <string>] [-h] [-i <file>] [-k <int>] [-a <string>]
[-m <file>] [-x <file>]
```

Given a contract-based decomposition it generates a heirarchical fault tree according with the approach desribed in "M. Bozzano, A. Cimatti, C. Mattarei, and S. Tonetta. Formal Safety Assessment via Contract-Based Design. In Proceedings of ATVA 2014. Sydney, Australia, November 3-7, 2014.".

The optional parameter "-x" enables the additional fault tree computation on leaves implementations by providing a fault injection xml file description.

Command Options:

`-C <string>`	Check just the specified contract, rather than all of them
`-h`	Shows a brief description of the available options.
`-i file`	Reads the OSS specification. If not specified, the command reads from standard input
`-k <int>`	with bmc: bound on length of path [default=10] with ic3 or kzeno: bound of underlying IC3 [default=10]

`-a <string>`	force algorithm type [default=auto] Valid values are: bmc, bdd, ic3, auto
`-m <file>`	Set a file with the mapping OSS component -¿ SMV file. Its format is: (¡OSS component name¿ ¡SMV filename¿)+ Equivalent to deprecated -a
`-x <file>`	XML file describing the fault extension.

7 OCRA Command Line Options

`-ocra-discrete-time`	Enables the interpretation of the model over discrete time instead of default hybrid time. The model must not contain: • continuous variables • der operator • time_until operator
`-ocra-old-smv-format`	Write and read SMV models with the format used before version 1.3.0
`-ocra-async-fairness`	Add to the specification the constraint that each subcomponent will eventually not stutter. It affects only models with asynchronous refinement.

References

[BCMT14] M. Bozzano, A. Cimatti, C. Mattarei, and S. Tonetta. Formal Safety Assessment via Contract-Based Design. In *ATVA*, 2014. To appear.

[CES] CESAR patterns. `http://www.cesarproject.eu/fileadmin/user_upload/CESAR_D_SP2_R2.2_M2_v1.000.pdf`.

[CRST12] A. Cimatti, M. Roveri, A. Susi, and S. Tonetta. Validation of Requirements for Hybrid Systems: a Formal Approach. *ACM Trans. Softw. Eng. Methodol.*, 21(4):22, 2012.

[CRT09] A. Cimatti, M. Roveri, and S. Tonetta. Requirements Validation for Hybrid Systems. In *CAV*, pages 188–203, 2009.

[CT] A. Cimatti and S. Tonetta. Contracts-refinement proof system for component-based embedded systems . *Sci. Comput. Program.* To appear.

[CT12] A. Cimatti and S. Tonetta. A Property-Based Proof System for Contract-Based Design. In *SEAA*, 2012.

[FoR] FoReVer project. `https://es.fbk.eu/index.php?n=Projects.FoReVer`.

[HyC] HyCOMP website. `https://es.fbk.eu/tools/hycomp/`.

[NuS] NuSMV3 website. `https://es.fbk.eu/tools/nusmv3/`.

[nuX] nuXmv website. `https://es.fbk.eu/tools/nuXmv/`.

[OCR] OCRA website. `https://es.fbk.eu/tools/ocra/`.

[Pnu77] A. Pnueli. The Temporal Logic of Programs. In *FOCS*, pages 46–57, 1977.

[Saf] SafeCer project. http://www.safecer.eu.

[SPE] SPEED project. http://www.speeds.eu.com/.

[XSA] xSAP website. https://es.fbk.eu/tools/xsap/.

A Concrete syntax

A.1 Othello System Specification

An Othello System Specification (OSS) is written following the grammar below (in Extended Backus-Naur Form):

```
OSS          = requirements? system_comp component* ;
requirements = "@requires" "discrete-time" | "@requires" "hybrid-time" ;
system_comp  = "COMPONENT" comptype? "system" interface refinement? ;
component    = "COMPONENT" comptype interface refinement? ;
interface    = "INTERFACE" var* contract* define*;
refinement   = "ASYNC"? "REFINEMENT" subcomponent* connection* refinedby* valid_prop*;
var          = port | parameter | operation ;
port         = ("IN" | "OUT")? "PORT" name ":" type ";" ;
parameter    = "PARAMETER" name ":" type | euf ";" ;
operation    = ("PROVIDED" | "REQUIRED") "OPERATION" "PORT"? name
               "(" op_parameter* ")" ":" (type | "void") ";" ;
op_parameter = ("IN" | "OUT")? name ":" type ;
define       = "DEFINE" name ":=" constraint ";"
type         = "boolean" | "integer" | "real" | "continuous" | "event" |
               "{" (number | name)+ "}" -- enumeration
               | number ".." number -- range
               | ("unsigned" | "signed")? "word" "[" number "]" ;
euf          = euf_subtype(\* euf_subtype)* -> euf_subtype ;
euf_subtype  = boolean | real | integer ;
contract     = "CONTRACT" name
               "assume" ":" constraint ";"
               "guarantee" ":" constraint ";" ;
subcomponent = "SUB" name ":" comptype ";" ;
connection   = "CONNECTION" name ":=" constraint ";"
formula      = "CONSTRAINT" constraint ";"
refinedby    = "CONTRACT" name "REFINEDBY" contr_id+ ";" ;
contr_id     = name "." name ;
valid_prop   = "CONSISTENCY" "NAME" name ":=" formula_id+; |
               "POSSIBILITY" "NAME" name ":=" (formula_id | contrain) "GIVEN" formula_id+ ";" |
               "ENTAILMENT"  "NAME" name ":=" (formula_id | contrain) "BY" formula_id+ ";" ;
formula_id   = name "." name "." ("ASSUMPTION" | "GUARANTEE" | "NORM_GUARANTEE") ;
```

where:

- `name` is a string;
- there cannot be two components with the same name;
- for every component, there cannot be two subcomponents with the same name;
- `comptype` is a string that matches one of the components' name;
- in the list of components forming the OSS, there exists a component whose name is `system`;
- the relationship that links a component to its subcomponents is not circular and form a tree rooted in the system component;
- the `constraint` in the definition of a `contract` in an `interface` must be an Othello constraint as defined above where every variable must match a variable of the interface;
- the `constraint` in the definition of a `connection` in the `refinement` of a `component` must be an Othello constraint as defined above where every variable must either match a port of the interface or be in the form `sub.var` where `sub` matches a subcomponent's name of the refinement and `var` matches a variable of the interface of such subcomponent;
- there cannot be two validation properties with the same name.

A.2 Othello Port Types

A.2.1 Boolean

The boolean type comprises symbolic values **FALSE** and **TRUE**. The **event** type has the same domain of the boolean type. The difference is that while a boolean port is evaluated in a state, an **event** is evaluated in a transition: we say that an **event** occurs during a transition if it is **TRUE** in that transition.

Accordingly, the values of event ports are listed in a separate "Transition" section in the OCRA counterexamples, between two "State" sections.

A.2.2 Enumeration Types

An enumeration type is a type specified by full enumerations of all the values that the type comprises. For example, the enumeration of values may be {`stopped, running, waiting, finished`}, {`2, 4, -2, 0`}, {`FAIL, 1, 3, 7, OK`}, etc. All elements of an enumeration have to be unique although the order of elements is not important. A range of whole numbers can be declared with `N..M`. For example the following declarations are equivalent:

```
2..5
{2, 3, 4, 5}
```

A.2.3 Word

The unsigned word[•] and signed word[•] types are used to model vector of bits (booleans) which allow bitwise logical and arithmetic operations (unsigned and signed, respectively). These types are distinguishable by their width. For example, type unsigned word[3] represents vector of three bits, which allows unsigned operations, and type signed word[7] represents vector of seven bits, which allows signed operations.

When values of unsigned word[N] are interpreted as integer numbers the bit representation used is the most popular one, i.e. each bit represents a successive power of 2 between 0 (bit number 0) and 2^{N-1} (bit number $N-1$). Thus unsigned word[N] is able to represent values from 0 to $2^N - 1$.

The bit representation of signed word[N] type is "two's complement", i.e., negative numbers are represented by 2^N minus their absolute value. Thus, the possible values for signed word[N] are from -2^{N-1} to $2^{N-1} - 1$.

A.2.4 Integer

The domain of the integer type is the set of integers. Note that the use of ports with integer type requires the usage of infinite-state model checking algorithms.

A.2.5 Real

The domain of the real type is the set of real numbers. Note that the use of ports with real type requires the usage of infinite-state model checking algorithms.

A.2.6 Continuous

The domain of the **continuous** type is the set of continuous and differentiable functions. They are used to represent a value that is a continuous function of time. Note that the use of ports with **continuous** type requires the usage of infinite-state model checking algorithms and is available only for the hybrid time mode of OCRA.

A.2.7 Array

Arrays are declared with a lower and upper bound for the index, and the type of the elements in the array. For example,

```
array 0..3 of boolean
array 10..20 of {OK, y, z}
```

array `1..8 of` array `-1..2 of` unsigned word[5]

The type array `1..8 of` array `-1..2 of` unsigned word[5] means an array of 8 elements (from 1 to 8), each of which is an array of 4 elements (from -1 to 2) that are 5-bit-long unsigned words.

Array subtype is the immediate subtype of an array type. For example, subtype of array `1..8 of` array `-1..2 of` unsigned word[5] is array `-1..2 of` unsigned word[5] which has its own subtype unsigned word[5].

Expression of array type can be constructed with variables of array type.

Internally, these arrays are treated as a set of variables.

A.2.8 Uninterpreted functions

In OCRA it is also possible to define uninterpreted functions. Only parameters can be declared with this type. These functions are rigid, i.e. their denotation does not change from two different time points. These functions can be seen as parameters: the denotation of the function is defined in the initial state and kept from that point on. Below is reported a simple example of declaring a function `funct1` that takes two reals as arguments, and returns an integer, and a function `funct2` that takes two reals and returns an unsigned word of size 32.

```
PARAMETER funct1 : real * real -> integer ;
PARAMETER funct2 : real * real -> unsigned word[32] ;
```

Note: Currently in OCRA we only support a limited number of data types both as return type and as type of each argument of a function. In particular, the supported types are: `boolean`, `real`, `integer`, and `word[N]`. Support for richer types (e.g. enumeratives, bouded integers and array) is ongoing.

A.3 Othello constraints[5]

An Othello constraint is written following the grammar below (in Extended Backus-Naur Form):

```
constraint    = atom |
                -- boolean operators
                "not" constraint |
                constraint "and" constraint |
                constraint "or" constraint |
                constraint "xor" constraint |
                constraint "implies" constraint |
                constraint "iff" constraint |
                -- temporal future operators
                "always" constraint |
                "never" constraint |
                "in the future" constraint |
                "then" constraint |
                constraint "until" constraint |
                constraint "releases" constraint |
                -- temporal past operators
                "historically" constraint |
                "in the past" constraint |
                "previously" constraint |
                constraint "since" constraint |
                constraint "triggered" constraint |
                ;
atom          = "TRUE" |
                "FALSE" |
                term relational_op term |
                "time_until" "(" term ")" relational_op term |
                term ;
term          = variable |
                constant |
                term "+" term |
                term "-" term |
                term "*" term |
                term "/" term |
                term "mod" term |
```

[5]The OCRA data types and operators are based on the NUXMV input language. See `https://es.fbk.eu/tools/nuxmv/downloads/nuxmv-user-manual.pdf` for a detailed description.

```
                term "[" index "]" | -- array indexing
                "der" "(" variable ")" |
                "next" "(" variable ")" |
                function "(" term(, term)* ")" | -- function call
                term "?" term ":" term | -- compact if then else
                "case" (term ":" term ";")+ "esac" | -- if then else
                count "(" term ("," term)* ")" | -- count of true boolean expressions
                -- word operators
                term ">>" term |  -- bit shift right
                term "<<" term |  -- bit shift left
                term "[" term ":" term "]" | -- word bits selection
                term "::" term | -- word concatenation
                sizeof "(" term ")" | -- word size as an integer
                extend "(" term "," term ")" | -- word width extension
                resize "(" term "," term ")" | -- word width resize
                signed word[N] "(" term ")" | -- integer to signed word conversion
                unsigned word[N] "(" term ")" | -- integer to unsigned word conversion
                -- set operators
                term "union" term |
                "{" term ("," term)"}" | -- set
                term "in" term | -- set membership
                -- cast operators
                word1 "(" term ")" | -- boolean to unsigned word[1] conversion
                bool "(" term ")" |
                toint "(" term ")" |
                swconst "(" term ")" | -- integer to signed word constant conversion
                uwconst "(" term ")" | -- integer to unsigned word constant conversion
                signed "(" term ")" | -- unsigned word to signed word conversion
                unsigned "(" term ")" | -- signed word to signed word conversion
                floor "(" term ")"
                ;

relational_op = ( "=" | "!=" | "<" | ">" | "<=" | ">=" ) ;
```

where:

- `constant` is a constant number;
- `variable` is a string.

B Abstract syntax and semantics

B.1 Abstract syntax and semantics of HRELTL constraints

B.1.1 Abstract syntax

The logic underlying Othello constraints is called HRELTL. HRELTL is built over a set of basic atoms, that are real arithmetic predicates over $V \cup \text{NEXT}(V)$, or over $V \cup \text{DER}(V)$, where V is a set of variables, $\text{NEXT}(V)$ the set of next variables and $\text{DER}(V)$ the set of derivatives.

The set $PRED$ is defined as the set of *linear arithmetic* predicates in one of the following forms:

- $a_0 + a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \sim 0$ where $v_1, \ldots, v_n \in V$, $a_0, \ldots, a_n$ are constants, and $\sim \in \{<, >, =, \leq, \geq, \neq\}$[6].
- $a_0 + a_1 \dot{v} \bowtie 0$ where $v \in V_C$, a_0, a_1 are arithmetic predicates over variables in V_D, and $\sim \in \{<, >, =, \leq, \geq, \neq\}$.

The HRELTL is defined as the extension of LTL defined with the following rules: if $p \in PRED$, ϕ_1 and ϕ_2 are HRELTL formulas, e is an event, $\sim \in \{<, >, =, \leq, \geq, \neq\}$ and c an arithmetic term, then:

- p is a HRELTL formula;
- $\neg\phi_1$, $\phi_1 \wedge \phi_2$, $\mathbf{X}\ \phi_1$, $\phi_1\ \mathbf{U}\ \phi_2$ are HRELTL formulas;
- $\triangleright_{\sim c} e$ is a HRELTL formula.

[6] As described in [CRT09], instead of constants, also discrete variables can be used, but the currently used SMT solver does not support non-linear constraints.

We use standard abbreviations for $\vee$, $\rightarrow$, $\mathbf{G}$, $\mathbf{F}$, $\mathbf{R}$ (see, e.g., [CRT09]). $\triangleright$ corresponds to "time_until". "never" is an abbreviation for $\mathbf{G}\ \neg$. The other abstract connectives correspond the the concrete ones used in the previous section in a straightforward way.

B.1.2 Semantics

HRELTL formulas are interpreted with hybrid traces, which are defined as follows. Let V be the finite disjoint union of the sets of variables V_D (with a discrete evolution) and V_C (with a continuous evolution). A state s is an assignment to the variables of V ($s : V \rightarrow \mathbb{R}$). We write Σ for the set of states. Let $f : \mathbb{R} \rightarrow \Sigma$ be a function describing a continuous evolution. We define the projection of f over a variable v, written f^v, as $f^v(t) \doteq f(t)(v)$. We say that a function $f : \mathbb{R} \rightarrow \mathbb{R}$ is piecewise analytic iff there exists a sequence of adjacent intervals $J_0, J_1, ... \subseteq \mathbb{R}$ and a sequence of analytic functions $h_0, h_1, ...$ such that $\cup_i J_i = \mathbb{R}$, and for all $i \in \mathbb{N}$, $f(t) = h_i(t)$ for all $t \in J_i$. Note that, if f is piecewise analytic, the left and right derivatives exist in all points. We denote with $\dot{f}$ the derivative of a real function f, with $\dot{f}(t)_-$ and $\dot{f}(t)_+$ the left and the right derivatives respectively of f in t. Let I be an interval of $\mathbb{R}$ or $\mathbb{N}$; we denote with $le(I)$ and $ue(I)$ the lower and upper endpoints of I, respectively. We denote with $\mathbb{R}^+$ the set of non-negative real numbers.

A hybrid trace over V is a sequence $\langle \overline{f}, \overline{I} \rangle \doteq \langle f_0, I_0 \rangle, \langle f_1, I_1 \rangle, \langle f_2, I_2 \rangle, \ldots$ such that, for all $i \in \mathbb{N}$,

- either I_i is an open interval ($I_i = (t, t')$ for some $t, t' \in \mathbb{R}^+$, $t < t'$) or is a singular interval ($I_i = [t, t]$ for some $t \in \mathbb{R}^+$);
- the intervals are adjacent, i.e. $ue(I_i) = le(I_{i+1})$;
- the intervals cover $\mathbb{R}^+$: $\bigcup_{i \in \mathbb{N}} I_i = \mathbb{R}^+$ (thus $I_0 = [0, 0]$);
- $f_i : \mathbb{R} \rightarrow \Sigma$ is a function such that, for all $v \in V_C$, f_i^v is continuous and piecewise analytic, and for all $v \in V_D$, f_i^v is constant;
- if $I_i = (t, t')$ then $f_i(t) = f_{i-1}(t)$, $f_i(t') = f_{i+1}(t')$.

We denote with $PRED$ the set of predicates, with p a generic predicate, with p_{curr} a predicate over V only, with p_{next} a predicate over V and $\text{NEXT}(V)$ containing at least an event variable or a next variable, and with p_{der} a predicate over V and $\text{DER}(V)$ containing at least a derivative variable. We denote with $\overline{p}$ the predicate obtained from p by replacing $<$ with $\geq$, $>$ with $\leq$, $=$ with $\neq$ and vice versa. We denote with $p_\sim$ the predicate obtained from p by substituting the top-level operator with $\sim$, for $\sim \in \{<, >, =, \leq, \geq, \neq\}$.

The HRELTL is interpreted over hybrid traces. The predicates p_{curr}, p_{next} and p_{der} are interpreted over hybrid traces as follows:

- $\langle \overline{f}, \overline{I} \rangle, i \models_p p_{curr}$ iff, for all $t \in I_i$, p_{curr} evaluates to true when v is equal to $f_i^v(t)$, denoted with $f_i(t) \models_p p$;
- $\langle \overline{f}, \overline{I} \rangle, i \models_p p_{next}$ iff there is a discrete step between i and $i+1$, i.e. $I_i = I_{i+1} = [t, t]$, and p_{next} evaluates to true when v is equal to $f_i^v(t)$ and $\text{NEXT}(v)$ to $f_{i+1}^v(t)$, denoted with $f_i(t), f_{i+1}(t) \models_p p_{next}$;
- $\langle \overline{f}, \overline{I} \rangle, i \models_p p_{der}$ iff, for all $t \in I_i$, p_{der} evaluates to true both when v is equal to $f_i^v(t)$ and $\text{DER}(v)$ to $\dot{f}_i^v(t)_+$, and when v is equal to $f_i^v(t)$ and $\text{DER}(v)$ to $\dot{f}_i^v(t)_-$, denoted with $f_i(t), \dot{f}_i(t)_+ \models_p p_{der}$ and $f_i(t), \dot{f}_i(t)_- \models_p p_{der}$ (when $\dot{f}_i(t)$ is defined this means that $f_i(t), \dot{f}_i(t) \models_p p_{der}$).

Finally, we can define the semantics of HRELTL:

- $\langle \overline{f}, \overline{I} \rangle, i \models p$ iff $\langle \overline{f}, \overline{I} \rangle, i \models_p p$;
- $\langle \overline{f}, \overline{I} \rangle, i \models \neg\phi$ iff $\langle \overline{f}, \overline{I} \rangle, i \not\models \phi$;
- $\langle \overline{f}, \overline{I} \rangle, i \models \phi \wedge \psi$ iff $\langle \overline{f}, \overline{I} \rangle, i \models \phi$ and $\langle \overline{f}, \overline{I} \rangle, i \models \psi$;
- $\langle \overline{f}, \overline{I} \rangle, i \models \mathbf{X}\ \phi$ iff there is a discrete step at i ($I_i = I_{i+1}$), and $\langle \overline{f}, \overline{I} \rangle, i+1 \models \phi$;

- $\langle \overline{f}, \overline{I} \rangle, i \models \phi \ \mathbf{U} \ \psi$ iff, for some $j \geq i$, $\langle \overline{f}, \overline{I} \rangle, j \models \psi$ and, for all $i \leq k < j$, $\langle \overline{f}, \overline{I} \rangle, k \models \phi$;
- $\langle \overline{f}, \overline{I} \rangle, i \models \rhd_{\sim c} \phi$ iff, for some $j \geq i$, $I_j = I_{j+1} = [t, t]$ and $\langle \overline{f}, \overline{I} \rangle, j \models \phi$ and, for all $i \leq k < j$, $\langle \overline{f}, \overline{I} \rangle, k \not\models \phi$ and for all $t' \in I_i, t - t' \sim c$;

B.1.3 Examples

The following formulas are examples of expressions with time-until: $G(p \rightarrow \rhd_{\leq 10} q)$: always the maximum delay between p and the next q is 10 time units; $\rhd_{\geq 5} p \wedge G(p \rightarrow \rhd_{=10} p)$: p happens exactly every 10 time units after an initial offset of 5 time units.

B.2 Abstract syntax and semantics of the system specification

A *component* S is described with a set V_S of ports, which are the variables representing the relevant information of the component that are visible from outside it. An *implementation* of a component S is defined as a subset of traces over V_S, i.e., a subset of Π_{V_S}. An *environment* of S is also defined as a subset of Π_{V_S} (since V_S are the the variables at the interface of S).

A *connection* γ over a set $\mathcal{S}_\gamma$ of components defines the possible interaction of the components. The semantics $[\![\gamma]\!]$ of a connection is defined as a subset of traces over $\bigcup_{S \in \mathcal{S}_\gamma} V_S$, i.e. $[\![\gamma]\!] \subseteq \Pi_{\bigcup_{S \in \mathcal{S}_\gamma} V_S}$.

A *decomposition* of a component S is is pair $\rho = \langle Sub_\rho, \gamma_\rho \rangle$ where:

- $Sub_\rho(S)$ is a set of subcomponents such that $Sub_\rho(S) \neq \emptyset$ and $S \notin Sub_\rho(S)$,
- $\gamma_\rho(S)$ is a connection over $\{S\} \cup Sub_\rho(S)$.

The implementation of a decomposed component S consists of the composition of the implementations of its sub-components $Sub_\rho(S)$. Namely, it is given by all the traces that are compatible with the subcomponents and their connection. Formally, if for every $S' \in Sub_\rho(S)$, $I_{S'}$ is the implementation of S', the implementation I_S of S induced by the decomposition ρ is defined as $\{\pi \in \Pi_{V_S} \mid \text{there exists } \pi_{S'} \in I_{S'} \text{ for every } S' \in Sub_\rho(S) \text{ such that } \pi \times \bigotimes_{S' \in Sub_\rho(S)} \pi_{S'} \in [\![\gamma_\rho(S)]\!]\}$. Similarly, the environment of a subcomponent $U \in Sub_\rho(S)$ is composed by the environment of S and by the sibling subcomponents of S. Formally, if E_S is the environment of S, the environment E_U of U induced by the decomposition ρ of S is defined as $\{\pi_U \in \Pi_{V_U} \mid \text{there exists } \pi_{S'} \in I_{S'} \text{ for every } S' \in Sub_\rho(S) \setminus \{U\} \text{ and } \pi \in E_U \text{ such that } \pi \times \bigotimes_{S' \in Sub_\rho(S)} \pi_{S'} \in [\![\gamma_\rho(S)]\!]\}$.

A *system* is defined by a tree of components. The root of the tree is called the system component. The leafs of the tree are called atomic (or basic or primitive) components. The tree structure is given by the decomposition of each non-atomic component. Thus, if we consider Sub^* as the transitive closure of the function Sub, then $S \notin Sub^*(S)$ for any S in the system architecture.

Note that we avoid to distinguish between component type and component instances to simplify the notation. Actually, the subcomponents of a component type may be instances of the same component type and the system is a component instance. We simply see two component instances as two distinct components with the same structure and renamed ports and subcomponents.

Given a component S, a contract for S is a pair $\langle A, G \rangle$ of assertions over V_S representing respectively an *assumption* and a *guarantee* for the component. Let $C = \langle A, G \rangle$ be a contract of S. Let I and E be respectively an implementation and an environment of S. We say that I is a implementation satisfying C iff $I \cap [\![A]\!] \subseteq [\![G]\!]$. We say that E is an environment satisfying C iff $E \subseteq [\![A]\!]$. We denote with $Imp(C)$ and with $Env(C)$, respectively, the implementations and the environments satisfying the contract C.

Two contracts C and C' are *equivalent* (denoted with $C \equiv C'$) iff they have the same implementations and environments, i.e., iff $Imp(C) = Imp(C')$ and $Env(C) = Env(C')$.

Contracts are used to specify the assumptions and guarantees of components in a system architecture. We denote with $\xi(S)$ the contracts of the component S.

Since the decomposition of a component S into subcomponents induces a composite implementation of S and composite environment for the subcomponents, it is necessary to prove that the decomposition is correct with regards to the contracts. In particular, it is necessary to prove that the composite implementation of S satisfies the guarantee of

S's contracts and that the composite environment of each subcomponent U satisfies the assumptions of U's contracts. We perform this verification compositionally only reasoning with the contracts of the subcomponent independently from the specific implementation of the subcomponents or specific environment of the composite component.

Given a component S and a decomposition $\rho = \langle Sub, \gamma \rangle$, a set of contracts $\mathcal{C} \subseteq \bigcup_{S' \in Sub(S)} \xi(S')$ is a refinement of C, written $\mathcal{C} \leq_\rho C$, iff the following conditions hold:

1. for any implementation I of S induced by the implementations $\{I_{S'}\}_{S' \in Sub(S)}$ of the sub-components of S and the decomposition ρ, if, for all $S' \in Sub(S)$, for all $C' \in \xi(S') \cap \mathcal{C}$, $I_{S'} \in Imp(C')$, then $I \in Imp(C)$ (i.e., the correct implementations of the sub-contracts form a correct implementation of C);

2. for every subcomponent S'' of S, for every contract $C'' \in \xi(S'') \cap \mathcal{C}$, for any environment E'' of S'' induced by the decomposition ρ, the environment E of S and the implementations $\{I_{S'}\}_{S' \in Sub(S) \setminus \{S''\}}$ of the sub-components of S, if $E \in Env(C)$ and, for all $S' \in Sub(S) \setminus \{S''\}$, for all $C' \in \xi(S') \cap \mathcal{C}$, $I_{S'} \in Imp(C')$, then $E'' \in Env(C'')$ (i.e., for each sub-contract C'', the correct implementation of the other sub-contracts and a correct environment of C form a correct environment of C'').

C Patterns

The Othello language is an expressive and complex language. This can be a problem for a user non specifically trained with the formal languages. On one side, it is possible to write contracts that do not represent the wanted requirement. On the other side, it can happen to write a specification that represents a unnecessary hard satisfiability problem.

For this reason, we list here several constraint patterns, mostly inspired by the SPEED [SPE] and CESAR [CES] projects. The list is the result of an analysis of the use cases developed so far both internally and with our partners in Safecer [Saf] and Forever [FoR] projects. With a few exceptions all those realistic contracts can be expressed using only these patterns.

P01: Initial condition

The condition that must hold in the initial state of the system. It is a common mistake to write such constraint instead of **`always`** `condition`.

```
condition
```

P02: Invariant

A good condition will always hold (typically the negation of condition represents some bad state).

```
always condition
```

It is equivalent to the CESAR pattern F3.

P03: Bounded Delay

Each time a certain event has occurred, another event will occur within a minimum delay and a maximum delay. Very useful to express reactions to signals (e.g. a safe state is entered each time an error has occurred).

```
always (event1 implies (
(time_until(event2) >= interval_lower_bound) and
(time_until(event2) <= interval_upper_bound)
))
```

It is equivalent to the CESAR pattern R3: `Delay between event1 and event2 within interval`

P04: Assured Reaction

If a certain event has occurred, another event will eventually occur. Used in discrete time models.

```
always (event1 implies [not] in the future event2)
```

Analogue to the CESAR pattern F1: **whenever** event1 **occurs** event2 [**does not**] **occur**[**s**]

P05: Timed Reaction

Equivalent to **Bounded Delay** with 0 as lower bound, listed here because it is commonly needed.

```
always (event1 implies [not] time_until(event2) <= interval_upper_bound)
```

Analogue to CESAR pattern F1[7].

Combination of patterns

Several times there will be the need to use more than one pattern in the same assertion. For achieving this, just connect them together through conjuction or disjunction:

```
pattern1 (and | or)
pattern2 (and | or)
...
patternN
```

The following provides a reference sheet.

P01: Initial condition

```
condition
```

P02: Invariant

```
always condition
```

P03: Bounded Delay

```
always (event1 implies (
(time_until(event2) >= interval_lower_bound) and
(time_until(event2) <= interval_upper_bound)
))
```

P04: Assured Reaction

```
always (event1 implies [not] in the future event2)
```

P05: Timed Reaction

```
always (event1 implies [not] time_until(event2) <= interval_upper_bound)
```

Combination of patterns

```
pattern1 (and | or)
pattern2 (and | or)
...
patternN
```

[7] As a technical note, notice that it not possible to express in Othello this CESAR pattern with a lower bound different from 0. The semantic of CESAR would be that event2 must occur during the interval and can occur before it. However, the current Othello language would force the event to not occur before the specified interval (as in **Bounded Delay**)